

BILLY J. WILLIAMS, OSB #901366

Acting United States Attorney

District of Oregon

JAMES E. COX, JR., OSB # 085653

Assistant United States Attorney

jim.cox@usdoj.gov

United States Attorney's Office

District of Oregon

1000 SW Third Ave., Suite 600

Portland, Oregon 97204-2902

Telephone: (503) 727-1026

Facsimile: (503) 727-1117

Attorneys for Defendant United States

UNITED STATES DISTRICT COURT

DISTRICT OF OREGON

DIANE ROARK,

Case No.: 6:12-CV-01354-MC

Plaintiff,

v.

UNITED STATES OF AMERICA,

Defendant.

**DECLARATION OF CHARLES E.¹
IN SUPPORT OF DEFENDANT'S
PROPOSED PLAN FOR RETURN
OF ELECTRONICALLY STORED
INFORMATION**

¹ Section 6 of the National Security Agency Act of 1959, 50 U.S.C. § 3605 (Pub. L. No. 86-36) authorizes the National Security Agency (NSA) to protect from public disclosure, among other categories of information, the names of its employees. The undersigned declarant occupies a non-public position with the NSA. Thus, the name of the declarant is referenced by first name, last initial. The Agency is prepared to provide the full name of the declarant in an *ex parte*, under seal filing should the Court so require.

I, Charles E., hereby make the following declaration under penalty of perjury pursuant to 28 U.S.C. § 1746. I make this declaration on personal knowledge and, if called upon to do so, I could and would competently testify to the following matters.

1. I am a Computer Forensic Examiner with the National Security Agency (NSA) and currently assigned within the Office of Counter Intelligence, Computer Forensic Investigations. I have been in this work role for approximately two and a half years and have since conducted approximately 110 digital media examinations relating to security and counterintelligence issues affecting NSA and/or National Security matters. Since 2011, I have successfully completed approximately 672 training hours relevant to computer forensics, computer incident response, and network security.

2. I have been informed that the Federal Bureau of Investigation (FBI) seized a personal hard disk drive (HDD) from plaintiff Diane Roark and created a raw image copy. I have utilized software to verify the file integrity of all images by confirming the hash values were consistent with acquisition values documented by the FBI Computer Analysis and Response Team originally tasked to image the aforementioned HDD.

3. The government has previously conducted and completed a return of Electronically Stored Information ("ESI") contained on hard drives at issue in the Rule 41(g) action in the District of Maryland, *Wiebe v. Nat'l Security*

Agency, et al., District of Maryland Case No. 1:11-cv-3245. The government proposes that the same procedure used to review ESI in the *Wiebe* case also be used in this case. This procedure involves (1) identification of electronic files to be reviewed for return, (2) review, and (3) production.

4. The first step in the process is to identify the types of files on the computer that are to be reviewed for return. Many of the files on a computer hard drive are system files that run the operating system or software on the computer. System files generally have no functionality as independent files. User-created files, on the other hand, are files created by a user of the computer, such as emails, word processing documents, spreadsheets, and photographs. The government proposes that it review for return all of the following common user created file types that may be located within Plaintiff's user profile on Plaintiff's computer hard drive:

1. .doc (Microsoft Word file format)
2. .ppt (Microsoft PowerPoint file format)
3. .xls (Microsoft Excel file format)
4. .mdb (Microsoft Access file format)
5. .pdf (Adobe Portable Document Format file format)
6. .txt (Plain Text file format)
7. .rtf (Microsoft Rich Text Format file format)
8. .jpg (JPEG Image file format)
9. .msg (Microsoft Outlook file format)
10. .eml(x) (Apple mail message file format)
11. .mpg (MPEG video file format)
12. .wav (Waveform Audio file format)
13. .wmv (Windows Media Video file format)
14. .avi (Microsoft Audio Video Interleave file format)
15. .cat (Quicken Software)

16. .html (HyperText Markup Language file format)
17. .htm (HyperText Markup Language file format)
18. .dbx (Outlook Express email file format)
19. .flv (Adobe Flash Video file format)
20. .mp3 (MP3 audio file format)
21. .zip (Compressed archive file)
22. .wma (Windows Media Audio file format)
23. .wpd (WordPerfect file format)

5. In addition, the government will also review for return the emails located within the AOL Personal File Cabinet (PFC) folders associated with Plaintiff's AOL email address.

6. Once the files to be reviewed are identified, these files will be reviewed for classified or protected information. The government proposes a two-step review process. The NSA has prepared a key word search list designed to identify files that may contain classified or protected information. In the first step of the process, the government will conduct an automated search of the files to be reviewed with this key word list, as well as any key word list that has been provided by the House Permanent Select Committee on Intelligence (HPSCI).

7. The second step of the process is a manual review of any files that return a "hit" from these key word lists. Any files that return a "hit" on the key word list prepared by NSA will be reviewed manually by NSA to determine if the file contains classified or protected information. Likewise, any files that return a "hit" on the key word list prepared by HPSCI will be

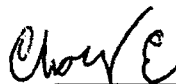
provided to HPSCI for HPSCI's determination if the file contains information protected under Plaintiff's non-disclosure agreement with HPSCI. (Any files that can only be reviewed manually – such as photographs – will be reviewed manually as well.)

8. Any files that contain classified, protected or HPSCI information will not be returned to Plaintiff. All other files within the scope of the review will be returned to Plaintiff. The government will copy these files onto a portable media (such as a CD or DVD), and deliver the portable media to Plaintiff. Many of these files will be in their “native” format and will be fully-functional if opened with the appropriate software (such as Microsoft Word). However, some of the less-common file formats – such as AOL email messages (“.pfc” extension files) – cannot be extracted from the hard drive in their native format. These files can only be returned as plain text files.

9. The government cannot provide an estimate for how long this review process will take because it does not know how many files must be manually reviewed. However, the government can provide an estimate once this information becomes available.

I declare under penalty of perjury that the foregoing is true and correct.

Executed this 28th day of May 2015 at Fort Meade, Maryland.



CHARLES E.

CERTIFICATE OF SERVICE

I hereby certify that a copy of the foregoing **Declaration of Charles E. in Support of Defendant's Proposed Plan for Return of Electronically Stored Information** was placed in a postage prepaid envelope and deposited in the United States Mail at Portland, Oregon on June 12, 2015, addressed to:

Diane Roark
2000 N. Scenic View Dr.
Stayton, OR 97383

And was sent via email to the following email address:

gardenofeden@wvi.com

/s/ Shari McClellan
SHARI McCLELLAN